U.S. Department of Justice

United States Attorney
District of New Hampshire

Federal Building
55 Pleasant Street, Room 352
Concord, New Hampshire 03301

603/225-1552

MEDIA RELEASE
For Immediate Release
January 23, 2004

Contact: **Thomas P. Colantuono**
United States Attorney
Arnold H. Huftalen
Assistant U. S. Attorney
(603) 225-1552

THREE MORE MEN PLEAD GUILTY IN NEW HAMPSHIRE WEB-BASED SOFTWARE PIRACY CONSPIRACY

CONCORD, NEW HAMPSHIRE: United States Attorney Tom Colantuono and Kenneth W. Kaiser, Special Agent in Charge of the Boston Division of the Federal Bureau of Investigation announced today that **JORDAN ZIELIN**, of Brooklyn, NY, **JOHN NEAS**, of Holbrook, MA and **KENNETH WOODS**, of Warrenton, VA, have pleaded guilty this week to charges that they each conspired with others to violate federal copyright laws through internet-based software piracy. All three defendants are scheduled to be sentenced in April and face a maximum sentence of five years in prison.

ZIELIN, **NEAS** and **WOODS** are the fourth, fifth and sixth individuals to be convicted in this software piracy conspiracy uncovered following a two-year undercover operation known as **"Operation Digital Piratez"** run in New Hampshire by the FBI's Boston-based Computer Squad. During the course of the undercover operation, agents and cooperating witnesses discovered several internet-based computer servers, known as "warez servers" run by groups of software pirates, and secret "Internet Relay Chat" channels used by those involved to communicate in real time about their software piracy activities. Warez servers exist for the exclusive illegal purpose of storing, copying, and reproducing, world-wide, copyright protected software. They serve no legitimate lawful purpose.

In December, 2001, the FBI executed search warrants, and obtained consent for additional searches, on computers located across the country. The servers involved in these three cases were known as ONLY THE FINEST WAREZ, which was being run at the Bank of America in Boston, MA by **ZIELIN**, without the bank's permission; CITY MORGUE, which was run out of a house in North Easton, MA by **NEAS**; and SHAYOL GHUL, which was run out of a Verio Data Center in Sterling, VA, by **WOODS**, without the company's knowledge or permission. Other servers, and the unauthorized locations from which they were operated, include: uNF (State of Nebraska Department of Roads); SCARECROW (Qwest Communications lab in Balston, VA); CORE DUMP (cable television company in Maryland); PORK CHOP EXPRESS (computer communications company in Brandon, FL); and LAND OF MILK AND HONEY

(Tulane University in New Orleans, LA). Another, known as WONDERLAND, was run out of an apartment in Ames, Iowa. The site operator of that server, **CHRISTOPHER MOTTER** of Ames, Iowa has already plead guilty here in New Hampshire and been sentenced to two years in federal prison.

ZIELIN admitted that he was the primary manager, or "site operator" as known within software piracy circles, for the warez server ONLY THE FINEST WAREZ, which was located at the Bank of America in Boston, MA. **ZIELIN** was an Information Technology support employee at the Bank of America and his criminal activity was conducted without the Bank's knowledge or permission. After it was seized and forensically examined by the FBI it was determined that there were over 100 illegal users who had access to the server and that it contained 400 gigabytes of pirated software. That is the equivalent of more than 275,000 three and one half inch floppy discs, filled to capacity. **NEAS** admitted he was a site operator for the server known as CITY MORGUE which had 81 illegal users and 400 gigabytes of pirated software. In addition to **NEAS**, **DANIEL McVAY**, of North Easton, MA, has already pleaded guilty here in New Hampshire as another site operator of that warez server. **WOODS** admitted that he physically placed, oversaw and maintained the server SHAYOL GHUL at his employer's place of business, a Verio Data Center in Sterling, VA. That server had 275 illegal users and 17 managers.

In order to ensure that the sites were accessible only to the conspirators, the site operators employed numerous security measures. These security measures included: 1) maintaining the warez site at a secret Internet Protocol address (the computer's address on the Internet, which all computers must use); 2) limiting access only to account holders; 3) providing account holders with a pre-arranged password, 4) allowing access to the warez site only from connecting computers with recognized, pre-registered IP addresses, and 5) using non-typical port connections. Each computer has 65,536 ports through which a connection can be made, and there are default ports for certain activities. However, these can be, and were, changed by the warez operators to afford greater secrecy. For example, ONLY THE FINEST WAREZ was set up to receive FTP traffic on port #1973, which is **ZIELIN'**s year of birth.

After the pleas of guilty were accepted by United States Chief Judge Paul Barbadoro and United States District Judge Steven McAuliffe, U.S. Attorney Tom Colantuono stated: "When the search warrants were executed in this case on December 11, 2001, Attorney General John Ashcroft characterized the operation as 'the most aggressive enforcement action to date against illegal software piracy' and 'a significant milestone in the efforts of U.S. law enforcement to work internationally to combat what is truly a global problem.' Now with the successful prosecution of these warez operators we have reached another milestone in our efforts to combat these crimes. I am proud of the work that has been undertaken in the District of New Hampshire to address Internet-based software piracy. Although these investigations and prosecutions are difficult and time consuming, we will not allow on-line criminals to prey on any sector of the business community, particularly software development businesses which are so important to this region. We, in conjunction with our partners at the FBI, will continue to hold those who abuse the Internet to violate the federal copyright laws responsible for their crimes."

The case was investigated by the Federal Bureau of Investigation Computer Squad in Boston, MA, and is being prosecuted by Assistant U.S. Attorney Arnold H. Huftalen with assistance from the U.S. Department of Justice ,Computer Crimes and Intellectual Property Section in Washington, D.C.